

FIG. 1  
[登録フェーズ]

被認証者  $U_B$   
(ユーザID=A、パスワード=S)

認証者  $U_A$

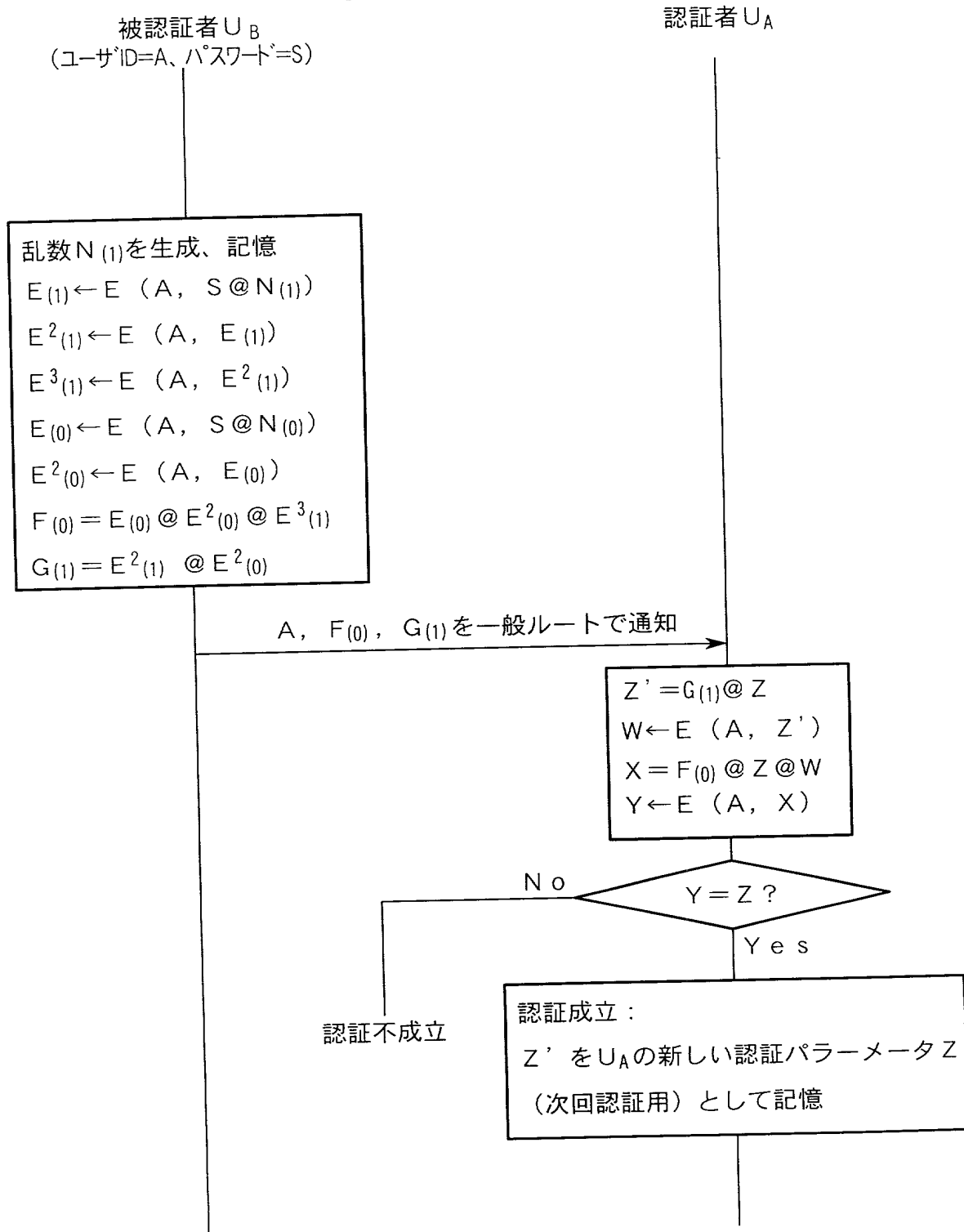
乱数  $N_{(0)}$  を生成、記憶  
 $E_{(0)} \leftarrow E(A, S @ N_{(0)})$   
 $E^2_{(0)} \leftarrow E(A, E_{(0)})$

$A, E^2_{(0)}$  をセキュアルートで通知

$Z = E^2_{(0)}$   
Z を  $U_A$  の認証パラメータ  
(初回認証用) として記憶

FIG. 2

[初回認証フェーズ]



# FIG. 3

[ k 回目認証フェーズ]

被認証者  $U_B$   
(ユーザID=A、パスワード=S)

認証者  $U_A$

乱数  $N_{(k)}$  を生成、記憶  
 $E_{(k)} \leftarrow E(A, S @ N_{(k)})$   
 $E^2_{(k)} \leftarrow E(A, E_{(k)})$   
 $E^3_{(k)} \leftarrow E(A, E^2_{(k)})$   
 $E_{(k-1)} \leftarrow E(A, S @ N_{(k-1)})$   
 $E^2_{(k-1)} \leftarrow E(A, E_{(k-1)})$   
 $F_{(k-1)} = E_{(k-1)} @ E^2_{(k-1)} @ E^3_{(k)}$   
 $G_{(k)} = E^2_{(k)} @ E^2_{(k-1)}$

A,  $F_{(k-1)}$ ,  $G_{(k)}$  を一般ルートで通知

$Z' = G_{(k)} @ Z$   
 $W \leftarrow E(A, Z')$   
 $X = F_{(k-1)} @ Z @ W$   
 $Y \leftarrow E(A, X)$

No  
 $Y = Z ?$   
 Yes

認証不成立

認証成立 :  
 $Z'$  を  $U_A$  の新しい認証パラメータ  $Z$   
 (k+1回目認証用) として記憶

FIG. 4

